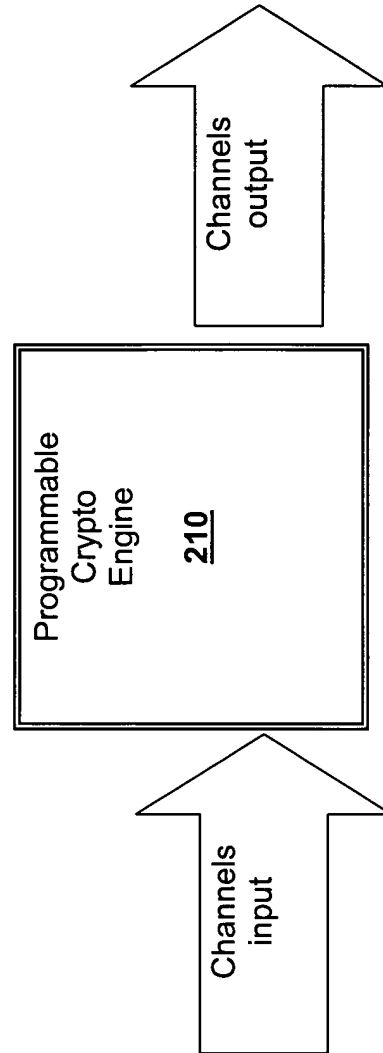


FIG. 1

FIG. 2A



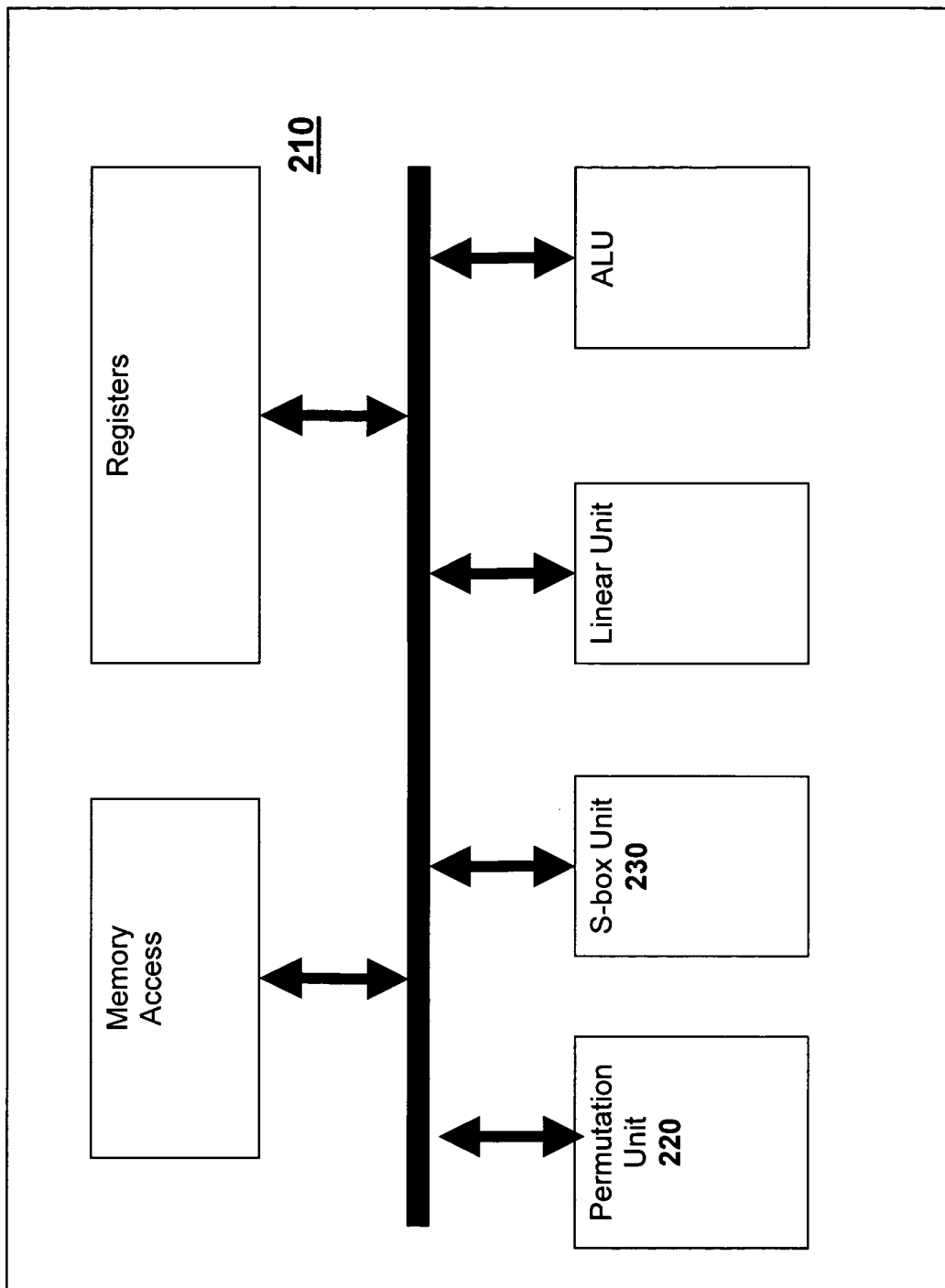


FIG. 2B

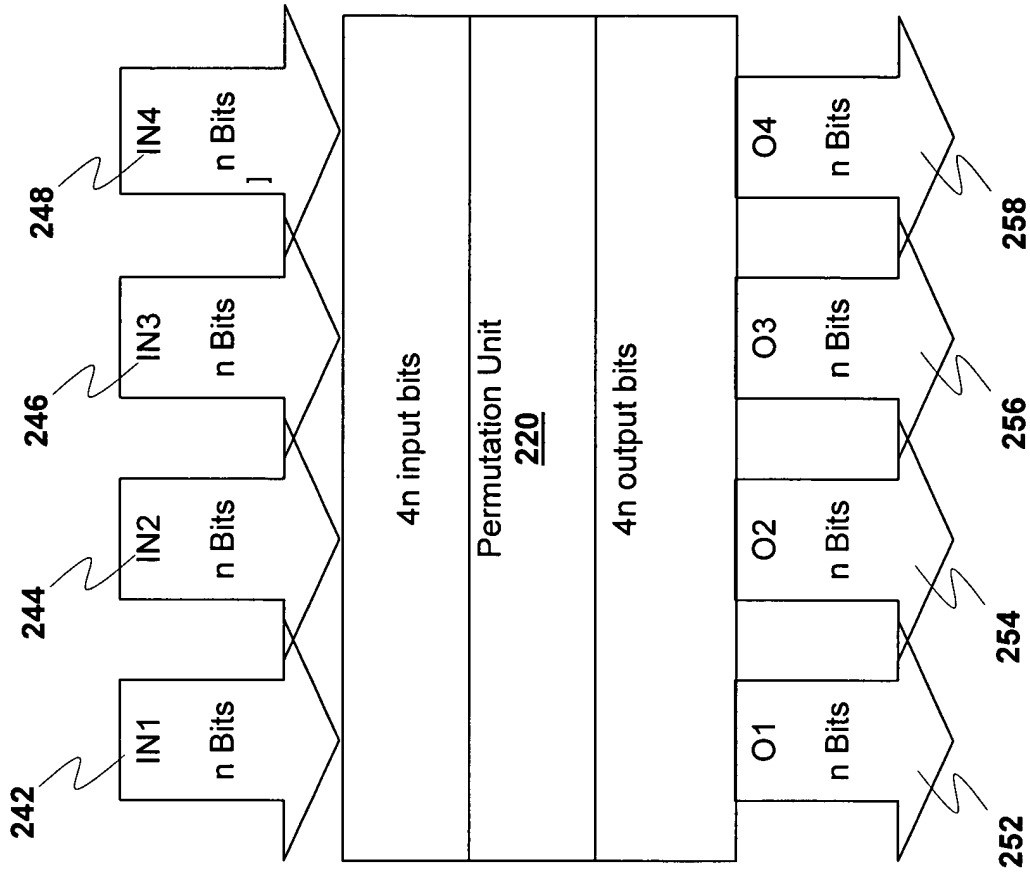
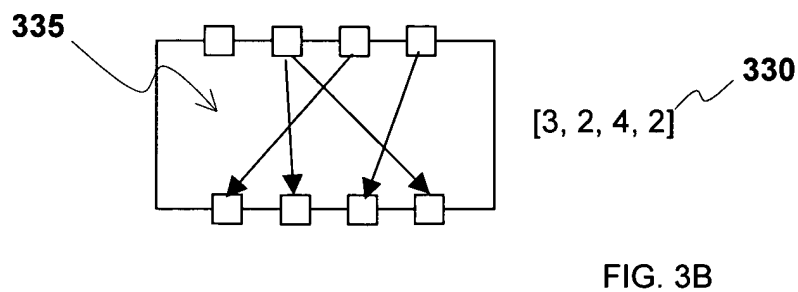
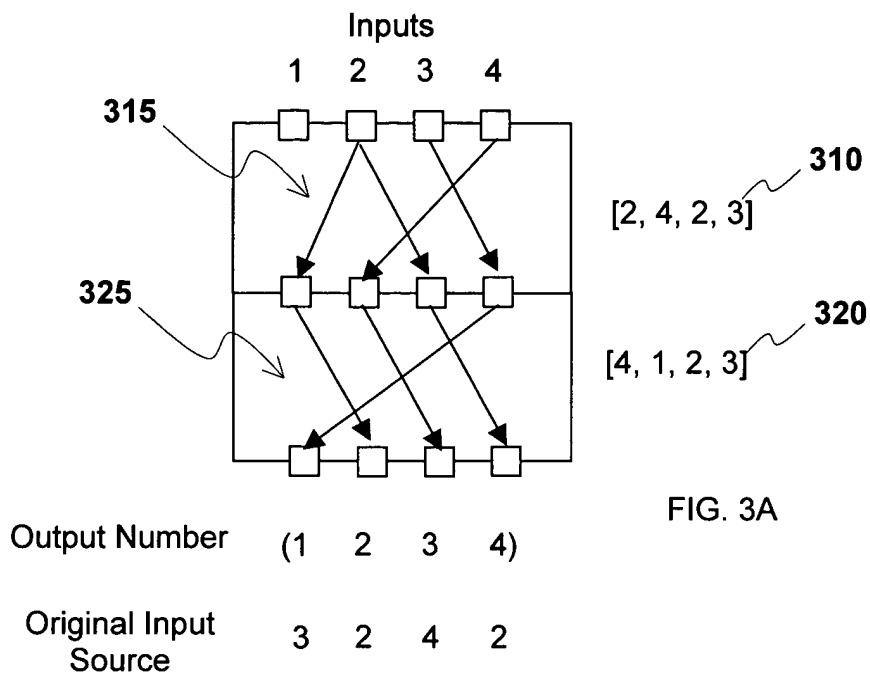


FIG. 2C



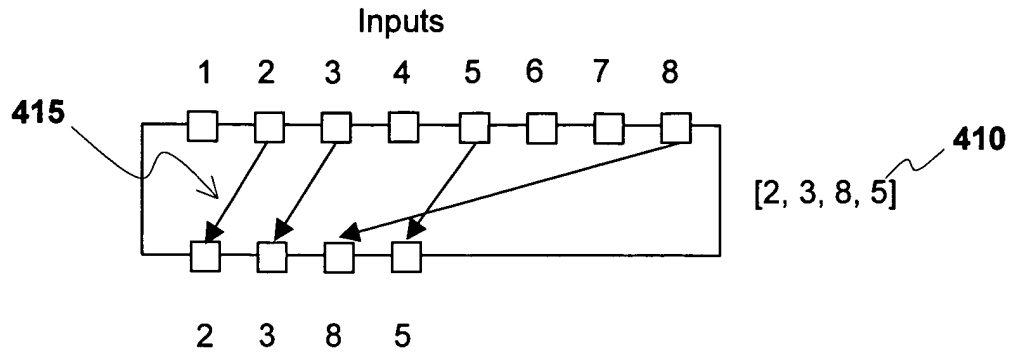


FIG. 4A

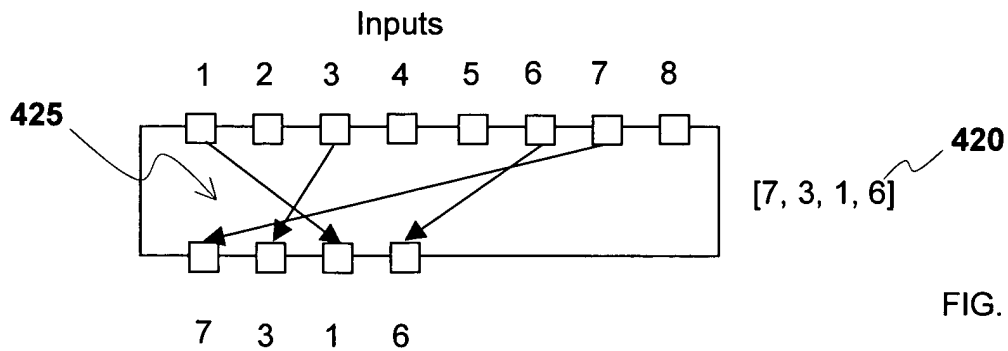


FIG. 4B

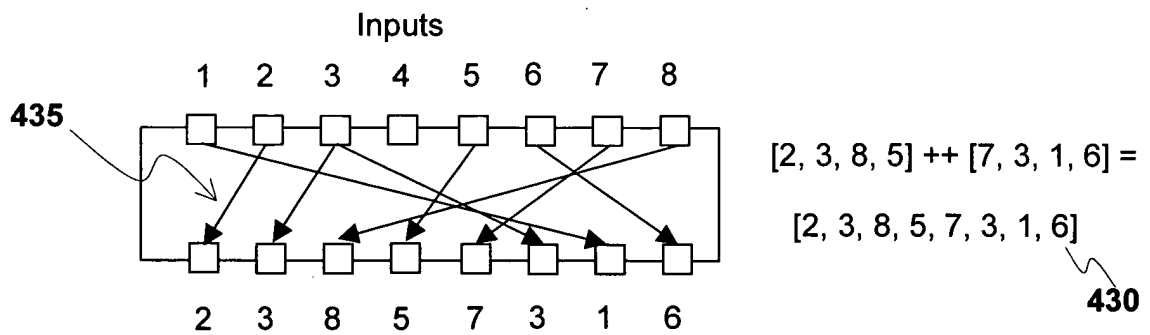
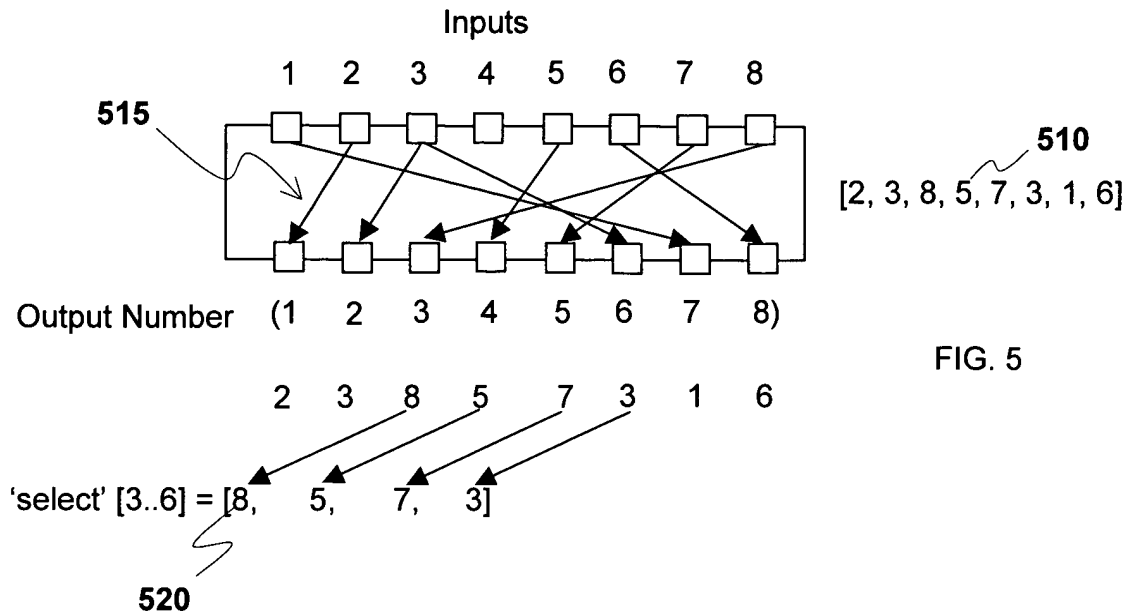
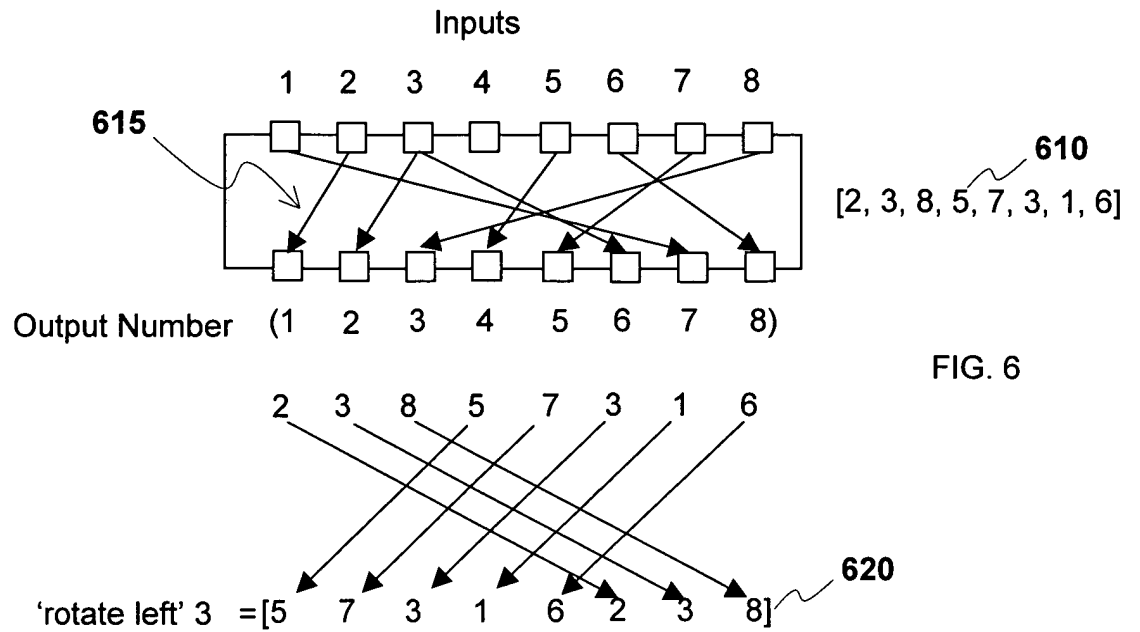
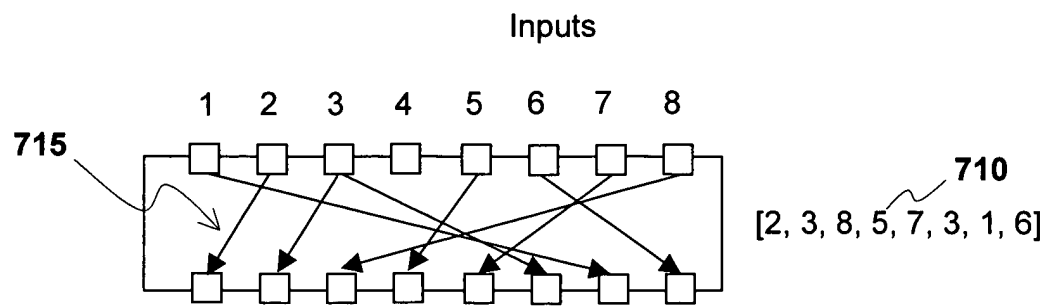


FIG. 4C







Permutation 2 3 8 5 7 3 1 6 ← 730

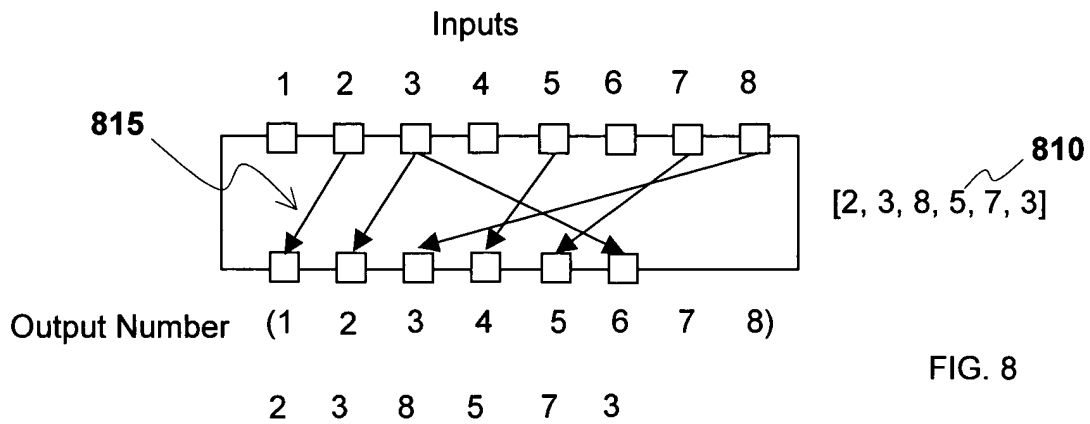
764 754

Output Position Number (1 2 3 4 5 6 7 8)

766 756

Inverse Permutation    7    1    2    1    4    8    5    3    ← 740

752    762    772



pad 8 [2, 3, 8, 5, 7, 3] = [1, 1, 2, 3, 8, 5, 7, 3]

↖
↖

842
844

910  
pu1 = PU {perm = 1,  
922 o1 = pad 16 (expansion `select` [1..8]),  
924 o2 = expansion `select` [17..32],  
926 o3 = in1,  
928 o4 = initialPerm `select` [33..48]}  
where  
932 initialPerm = (in3 ++ in4) `into` desIP  
934 expansion = (initialPerm `select` [33..48]) `into`  
desE  
  
desE = [32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9,  
8, 9, 10, 11, 12, 13, 12, 13, 14, 15, 16, 1]

FIG. 9

FIG. 10

PERM1 =

[O1_31(IN4_16),	O2_31(IN2_31),	O3_31(IN3_31),	O4_31(IN1_31),
O1_30(IN4_25),	O2_30(IN2_30),	O3_30(IN3_30),	O4_30(IN1_30),
O1_29(IN4_12),	O2_29(IN2_29),	O3_29(IN3_29),	O4_29(IN1_29),
O1_28(IN4_11),	O2_28(IN2_28),	O3_28(IN3_28),	O4_28(IN1_28),
O1_27(IN4_3),	O2_27(IN2_27),	O3_27(IN3_27),	O4_27(IN1_27),
O1_26(IN4_20),	O2_26(IN2_26),	O3_26(IN3_26),	O4_26(IN1_26),
O1_25(IN4_4),	O2_25(IN2_25),	O3_25(IN3_25),	O4_25(IN1_25),
O1_24(IN4_15),	O2_24(IN2_24),	O3_24(IN3_24),	O4_24(IN1_24),
O1_23(IN4_31),	O2_23(IN2_23),	O3_23(IN3_23),	O4_23(IN1_23),
O1_22(IN4_17),	O2_22(IN2_22),	O3_22(IN3_22),	O4_22(IN1_22),
O1_21(IN4_9),	O2_21(IN2_21),	O3_21(IN3_21),	O4_21(IN1_21),
O1_20(IN4_6),	O2_20(IN2_20),	O3_20(IN3_20),	O4_20(IN1_20),
:			
:			
O1_2(IN4_21),	O2_2(IN2_2),	O3_2(IN3_2),	O4_2(IN1_2),
O1_1(IN4_28),	O2_1(IN2_1),	O3_1(IN3_1),	O4_1(IN1_1),
O1_0(IN4_7),	O2_0(IN2_0),	O3_0(IN3_0),	O4_0(IN1_0)];

FIG. 11

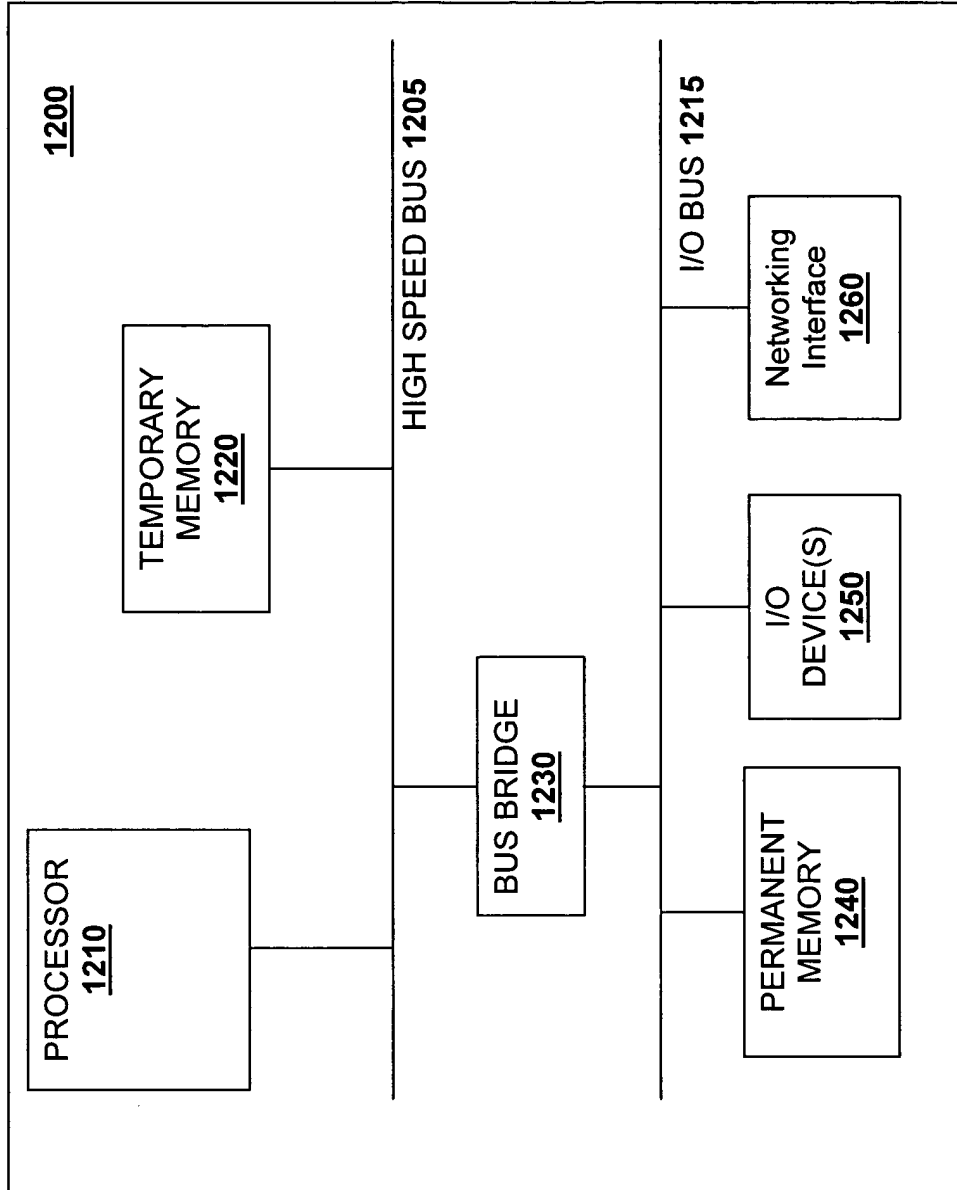


FIG. 12